Amendments to the Claims

Claim 1 (currently amended): A computer program product for providing fine-grained, identity-based access control in a computer networking environment, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for establishing a first security association between a first host and a boundary device, wherein the first security association uses strong cryptographic techniques;

computer-readable program code means for establishing a second security association between a second host and the boundary device, wherein the second security association uses strong cryptographic techniques;

computer-readable program code means for providing secure communications between a security enforcement function in the boundary device and an access control function;

computer-readable program code means for extracting, by the security enforcement function, a first authenticated identity associated with the first host during operation of the computer-readable program code means for establishing the first security association;

computer-readable program code means for extracting, by the security enforcement function, a second authenticated identity associated with the second host during operation of the computer-readable program means for establishing the second security association;

computer-readable program code means for providing the extracted first authenticated identity and the extracted second authenticated identity, by the security enforcement function, to the access control function; and

computer-readable program code means for determining access privileges of the first host

and the second host, by the access control function, based upon the provided extracted identities.

Claim 2 (original): The computer program product according to Claim 1, wherein the strong cryptographic techniques used for the first security association and the second security association are provided by protocols known as Internet Key Exchange and IP (Internet Protocol) Security Protocol.

Claim 3 (currently amended): The computer program product according to Claim 1, further comprising:

computer-readable program code means for securely making the determined access privileges available to the security enforcement function; and

computer-readable program code means for using the made-available access privileges to determine whether to forward a packet flowing between the first host and the second host using the first and second security associations or to discard the packet.

Claim 4 (currently amended): The computer program product according to Claim 1, further comprising:

computer-readable program code means for securely communicating packet-handling directives from the access control function to the security enforcement function, based upon the determined access privileges; and

computer-readable program code means for using the communicated packet-handling directives to determine whether to forward a packet flowing between the first host and the second

host using the first and second security associations or to discard the packet.

Claim 5 (original): The computer program product according to Claim 1, wherein the computer-readable program code means for providing secure communications further comprises computer-readable program code means for establishing a secure channel between the security enforcement function and the access control function.

Claim 6 (original): The computer program product according to Claim 1, wherein the first security association specifies only coarse-grained access control information.

Claim 7 (original): The computer program product according to Claim 1, wherein the first authenticated identity associated with the first host is an identification of a user of the first host.

Claim 8 (original): The computer program product according to Claim 1, wherein the first authenticated identity associated with the first host is an identification of an application executing on the first host.

Claim 9 (original): The computer program product according to Claim 1, wherein the second security association specifies only coarse-grained access control information.

Claim 10 (original): The computer program product according to Claim 1, wherein the second authenticated identity associated with the second host is an identification of a user of the second host.

Claim 11 (original): The computer program product according to Claim 1, wherein the second authenticated identity associated with the second host is an identification of an application executing on the second host.

Claim 12 (original): A system for providing fine-grained, identity-based access control in a computer networking environment, comprising:

means for establishing a first security association between a first host and a boundary device, wherein the first security association uses strong cryptographic techniques;

means for establishing a second security association between a second host and the boundary device, wherein the second security association uses strong cryptographic techniques;

means for providing secure communications between a security enforcement function and an access control function;

means for extracting, by the security enforcement function, a first authenticated identity associated with the first host during operation of the means for establishing the first security association;

means for extracting, by the security enforcement function, a second authenticated identity associated with the second host during operation of the means for establishing the second security association;

means for providing the extracted first authenticated identity and the extracted second authenticated identity, by the security enforcement function, to the access control function; and

means for determining access privileges of the first host and the second host, by the

access control function, based upon the provided extracted identities.

Claim 13 (original): The system according to Claim 12, wherein the strong cryptographic techniques used for the first security association and the second security association are provided by protocols known as Internet Key Exchange and IP (Internet Protocol) Security Protocol.

Claim 14 (currently amended): The system according to Claim 12, further comprising:

means for securely making the determined access privileges available to the security enforcement function; and

means for using the made-available access privileges to determine whether to forward a packet flowing between the first host and the second host using the first and second security associations or to discard the packet.

Claim 15 (currently amended): The system according to Claim 12, further comprising:

means for securely communicating packet-handling directives from the access control function to the security enforcement function, based upon the determined access privileges; and

means for using the communicated packet-handling directives to determine whether to forward a packet flowing between the first host and the second host using the first and second security associations or to discard the packet.

Claim 16 (original): The system according to Claim 12, wherein the security enforcement function operates in the boundary device, and wherein the means for providing secure

communications further comprises means for establishing a secure channel between the security enforcement function and the access control function.

Claim 17 (original): The system according to Claim 12, wherein the security enforcement function operates in the first host and in the second host, and wherein the means for providing secure communications further comprises means for establishing secure channels between the security enforcement function in the first and second hosts and the access control function.

Claim 18 (original): The system according to Claim 12, wherein the first authenticated identity associated with the first host is an identification of a user of the first host and/or an application executing on the first host.

Claim 19 (original): The system according to Claim 12, wherein the second authenticated identity associated with the second host is an identification of a user of the second host and/or an application executing on the second host.

Claim 20 (original): A method for providing fine-grained, identity-based access control in a computer networking environment, comprising steps of:

establishing a first security association between a first host and a boundary device, wherein the first security association uses strong cryptographic techniques;

establishing a second security association between a second host and the boundary device, wherein the second security association uses strong cryptographic techniques;

providing secure communications between a security enforcement function and an access control function;

extracting, by the security enforcement function, a first authenticated identity associated with the first host during operation of the step of establishing the first security association;

extracting, by the security enforcement function, a second authenticated identity associated with the second host during operation of the step of establishing the second security association;

providing the extracted first authenticated identity and the extracted second authenticated identity, by the security enforcement function, to the access control function; and

determining access privileges of the first host and the second host, by the access control function, based upon the provided extracted identities.

Claim 21 (original): The method according to Claim 20, wherein the strong cryptographic techniques used for the first security association and the second security association are provided by protocols known as Internet Key Exchange and IP (Internet Protocol) Security Protocol.

Claim 22 (currently amended): The method according to Claim 20, further comprising steps of:

securely making the determined access privileges available to the security enforcement function; and

using the made-available access privileges to determine whether to forward a packet flowing between the first host and the second host using the first and second security associations or to discard the packet.

Claim 23 (currently amended): The method according to Claim 20, further comprising steps of:

securely communicating packet-handling directives from the access control function to the security enforcement function, based upon the determined access privileges; and

using the communicated packet-handling directives to determine whether to forward a packet flowing between the first host and the second host using the first and second security associations or to discard the packet.

Claim 24 (original): The method according to Claim 20, wherein the security enforcement function operates in the boundary device, and wherein the step of providing secure communications further comprises the step of establishing a secure channel between the security enforcement function and the access control function.

Claim 25 (original): The method according to Claim 20, wherein the security enforcement function operates in the first host and in the second host, and wherein the step of providing secure communications further comprises the step of establishing secure channels between the security enforcement function in the first and second hosts and the access control function.

Claim 26 (original): The method according to Claim 20, wherein the first authenticated identity associated with the first host is an identification of a user of the first host and/or an application executing on the first host.

Claim 27 (original): The method according to Claim 20, wherein the second authenticated identity associated with the second host is an identification of a user of the second host and/or an application executing on the second host.

Claim 28 (currently amended): A method for providing fine-grained, identity-based access control in a computer networking environment, comprising steps of:

establishing a first security association between a first host and a first boundary device using strong cryptographic techniques;

establishing a second security association between a second host and a second boundary device using strong cryptographic techniques;

establishing a third security association between the first boundary device and the second boundary device using strong cryptographic techniques;

providing secure communications between a first security enforcement function operating in the first boundary device and an access control function;

providing secure communications between a second security enforcement function operating in the second boundary device and the access control function;

extracting, by the first security enforcement function, a first authenticated identity associated with the first host during operation of the step of establishing the first security association;

extracting, by the second security enforcement function, a second authenticated identity associated with the second host during operation of the step of establishing the second security association;

providing the extracted first authenticated identity and the extracted second authenticated identity, by the first and second security enforcement functions, to the access control function over the secure communications; and

determining access privileges of the first host and the second host, by the access control function, based upon the provided extracted identities.

Claim 29 (original): The method according to Claim 28, wherein the strong cryptographic techniques used for the first security association and the second security association are provided by protocols known as Internet Key Exchange and IP (Internet Protocol) Security Protocol.

Claim 30 (currently amended): The method according to Claim 28, further comprising steps of:

securely making the determined access privileges of the first host and second host available to the first and second security enforcement ~~function~~ functions, respectively; and

using the made-available access privileges to determine whether to forward a packet flowing between the first host and the second host using the first, second, and third security associations or to discard the packet.

Claim 31 (currently amended): The method according to Claim 28, further comprising steps of:

securely communicating packet-handling directives from the access control function to the first and second security enforcement ~~function~~ functions, based upon the determined access privileges; and

using the communicated packet-handling directives to determine whether to forward a

packet flowing between the first host and the second host or to discard the packet.

Claim 32 (canceled)

Claim 33 (currently amended): The method according to Claim 28, ~~wherein the first security enforcement function operates in the first host and the second security enforcement function operates in the second host, and~~ wherein:

the step of providing secure communications between the first security enforcement function and the access control function further comprises the step of establishing a first secure channel between the first security enforcement function and the access control function; and

the step of providing secure communications between the second security enforcement function and the access control function further comprises the step of establishing a second secure channel between the second security enforcement function and the access control function.

Claim 34 (original): The method according to Claim 28, wherein the first authenticated identity associated with the first host is an identification of a user of the first host and/or an application executing on the first host.

Claim 35 (original): The method according to Claim 28, wherein the second authenticated identity associated with the second host is an identification of a user of the second host and/or an application executing on the second host.

Claim 36 (currently amended): A method for providing fine-grained, identity-based access control in a computer networking environment, comprising steps of:

establishing a mutually-authenticated connection between a first end device and a second end device using strong cryptographic techniques, wherein the mutually-authenticated connection comprises a first mutually-authenticated network segment between the first end device and a boundary device providing network-layer protection and a second mutually-authenticated network segment between the second end device and the boundary device;

extracting a first authenticated identity associated with the first end device and a second authenticated identity associated with the second ~~host~~ end device during the step of establishing the mutually-authenticated connection;

providing secure communications between a security enforcement function operating in the boundary device and an access control function;

providing the extracted first and second authenticated identities, by the security enforcement function, to the access control function;

determining access privileges of the first end device and the second end device, by the access control function, based upon the provided extracted identities; ~~and~~

securely communicating packet-handling directives from the access control function to the security enforcement function, based upon the determined access privileges; and

using the packet-handling directives, by the security enforcement function, to determine whether to forward packets sent by the first end device on the first network segment to the second end device on the second network segment.

Claim 37 (added): The method according to Claim 28, wherein the first security enforcement function operates in the first host instead of in the first boundary device and the second security enforcement function operates in the second host instead of in the second boundary device.